Acta Sci. Math., 41 (1979), 133—136

Multiplicative periodicity in rings

REYADH R. KHAZAL

A well known result of JACOBSON [4] establishes that a ring R is commutative if for every $a\in R$ there is an integer $n>1$ (depending on a) such that $a=a^n$. This has been generalized by HERSTEIN [1]. On the other hand, ISKANDER [3] characterizes via polynomial identities varieties of rings in which every element generates a finite subring, while KRUSE [5] and L'VOV [6, 7] characterize via polynomial identities varieties generated by finite rings.

In the present paper we consider rings in which every element generates a finite multiplicative semigroup. It turns out that such rings are precisely the rings in which a power of every element generates a finite subring. A semigroup is called *periodic* if every element is of finite order. We call a ring R *periodic* if for every $a\in R$ there are a positive integer r and a polynomial $h(t)$ with integral coefficients such that $a^r+a^{r+1}h(a)=0$. The term "periodic" has been used in literature for the case $r=1$, (cf. OSBORN [8]). We will use the term periodic to mean also the case $r>1$. The main result is:

Theorem 1. *The following statements about a ring R are equivalent:*

(i) *R is periodic;*

(ii) *if $a\in R$ then a power of a generates a finite subring;*

(iii) *the multiplicative semigroup of R is periodic.*

It is clear that (ii) implies (iii) and (iii) implies (i). Before we show that (i) implies (ii) we give some preliminaries.

Theorem 2. (HERSTEIN [2]) *If R is a ring with centre C such that for every $a\in R$ there exists a polynomial $p_a(t)$ such that $a^2p_a(a)-a\in C$, then R is commutative.*

Proposition 3. *If R is a periodic division ring then R is a field. Also R is an algebraic extension of $\mathbf{Z}_p$ (the integers modulo p) for some prime p.*

Proof. Let $a\in R$. As R is periodic, there are $r>0$ and a polynomial $h(t)$ such that $a^r+a^{r+1}h(a)=0$. Thus $a^{r-1}(a+a^2h(a))=0$. But R is a division ring, hence $a+a^2h(a)=0$. Thus, by Herstein's Theorem 2, R is commutative. Since

Received November 4, 1977.

$\mathbf{Z}$, the ring of integers, is not periodic ($2+2^2h(2)=0$ is impossible), the prime field of R is $\mathbf{Z}_p$ for some prime p and so R is an algebraic extension of $\mathbf{Z}_p$.

Proposition 4. *Let R be a primitive ring. If R is periodic then R is isomorphic to a dense ring of algebraic linear transformations of a vector space V over a field F that is an algebraic extension of some prime field $\mathbf{Z}_p$.*

Proof. By Jacobson's Density Theorem R is isomorphic to a dense ring of linear transformations of a vector space V over a division ring D. However D is a homomorphic image of a subring of R. Hence D is periodic and thus D is a fieldt which is also an algebraic extension of $\mathbf{Z}_p$. In this case periodicity implies tha, the linear transformations involved are algebraic over $\mathbf{Z}_p$.

Proposition 5. *Let R be a periodic ring. Then*

(i) *$J(R)$ (the Jacobson radical of R) is nil;*

(ii) *$R/J(R)$ is isomorphic to a subdirect sum of dense rings of algebraic linear transformations of vector spaces over fields each of which is an algebraic extension of $\mathbf{Z}_p$ for some prime p.*

Proof. Statement (ii) follows from Proposition 4 and Jacobson's Structure Theorem [2, 4]. Let $a\in J(R)$. Then $a^r+a^{r+1}h(a)=0$ for some positive integer r and $h(t)\in\mathbf{Z}[t]$. Hence, $a^r=-a^{r+1}h(a)=a^{r+1}g(a)=a^{r+2}g(a)^2=a^{2r}g(a)^r$, and $(ag(a))^r$ is an idempotent. Hence $a^rg(a)^r=0$, as the only idempotent in $J(R)$ is 0. Hence $a^r=a^ra^rg(a)^r=0$ and $J(R)$ is nil.

The converse of Proposition 5 is not true. The ring of integers $\mathbf{Z}$ is a subdirect sum of $\mathbf{Z}_p$ for all primes p and $\mathbf{Z}$ is not periodic.

Proposition 6. *The following conditions on a ring R are equivalent:*

(i) *R is periodic;*

(ii) *every subring of R generated by one element is an extension of a nilpotent ring by a finite direct sum of finite fields;*

(iii) *every subring of R generated by one element is an extension of a nil ring by a finite ring;*

(iv) *for every $a\in R$ there are integers $s, t>1$ such that $(a-a^s)^t=0$.*

Proof. It is obvious that (ii) implies (iii) and (iv) implies (i). Let A be the subring of R generated by $a\in A$. Then every ideal of A is finitely generated as A is commutative and is generated by one element. If R is periodic then $J(A)$ is nil (by Proposition 5) and hence nilpotent. $A/J(A)$ is isomorphic to a subdirect sum of periodic primitive rings generated by one element. Thus $A/J(A)$ is isomorphic to a subdirect sum of finite fields $F(i)$. $F(i)$ is generated by one element a_i. Also $a_i^r+a_i^{r+1}h(a_i)=0$. But $a_i^{r-1}=0$ is impossible in $F(i)$, so $a_i+a_i^2h(a_i)=0$. Hence $e_i=-a_ih(a_i)$ is idempotent $\neq 0$ and it is the identity element of $F(i)$. Thus $\bar{a}=a+J(A)$ satisfies $\bar{a}+\bar{a}^2h(\bar{a})=0$ in $A/J(A)$ and $e=-\bar{a}h(\bar{a})$ is the identity

element of $A/J(A)$. Thus $A/J(A)$ is isomorphic to a finite direct sum of finite fields. This establishes that (i) implies (ii).

Let N be a nil ideal in A such that $A/N=F$ is finite. Hence F is periodic and is generated by one element. By (ii), $J(F)$ is nilpotent and $F/J(F)\cong F(1)\oplus\ldots\oplus F(k)$, where $F(i)$ is a finite field of characteristic p_i, $1\leqq i\leqq k$. Thus there is $s>1$ such that $F/J(F)$ satisfies $x-x^s=0$. Thus $\bar{a}=a+N$ satisfies $\bar{a}-\bar{a}^s\in J(F)$. As $J(F)$ is nilpotent, there is a positive integer r such that $(\bar{a}-\bar{a}^s)^r=0$, i.e. $(a-a^s)^r\in N$. Thus for some $t>0$, $(a-a^s)^{rt}=0$. This establishes that (iii) implies (iv) and concludes the proof of Proposition 6.

Now, we conclude the proof of Theorem 1. By Statement (ii) of Proposition 6, if $a\in R$ then $J(A)$ is nilpotent and $A/J(A)\cong F(1)\oplus\ldots\oplus F(k)$ where $F(i)$ is a finite field of characteristic p_i, $1\leqq i\leqq k$. Thus $ma\in J(A)$, where $m=$l.c.m. $(p_1, \ldots, p_k)$. Hence $(ma)^r=0$ for some $r>0$. Thus for every $a\in R$ some power a^r is torsion in the additive group of R. By (iv) of Proposition 6, $(b-b^s)^t=0$, $b=a^r$. b^{st} is a polynomial of degree less than st in b, and $nb=0$ for some $n>0$. In the subring B of R generated by b, every element has an expression in the form $\sum\{s_ib^i: 1\leqq i\leqq st, 0\leqq s_i<n\}$. Hence B is finite, it has at most n^{st-1} elements. Thus Statement (i) of Theorem 1 implies Statement (ii). This concludes the proof of Theorem 1.

If R is a periodic ring and $a\in R$, we define: Index $(a)=\inf\{r: r>0,\ a^r+ +a^{r+1}h(a)=0,\ h(t)\in\mathbf{Z}[t]\}$, Index $(R)=\sup\{\text{Index }(a): a\in R\}$, $N(R)=\sup\{n: n>0,$ for some $a\in R$, a is nilpotent, $a^n=0$ and $a^{n-1}\neq 0\}$. Degree $(a)=\inf\{\deg h(a): a^r+ +a^{r+1}h(a)=0,\ r>0,\ h(t)\in\mathbf{Z}[t]\}$. Degree $(R)=\sup\{\text{Degree }(a): a\in R\}$.

It turns out that

Proposition 7. *If R is a periodic ring then* $N(R)=\text{Index }(R)$.

Proof. Clearly, $N(R)\leqq\text{Index }(R)$. If $a\in R$ then by Proposition 6 (iv), $(a-a^s)^r=0$. One can assume that $r\leqq N(R)$. But Index $(a)\leqq r\leqq N(R)$. Hence Index $(R)\leqq N(R)$.

We conclude this paper by establishing some properties of periodic rings of bounded Index or Degree.

Proposition 8. *Let F be a periodic field. Then* Degree $(F)=d$ *iff* $F\cong GF(p, d+1)$ *(where $GF(p, t)$ is the Galois field of p^t elements).*

Proof. If F is periodic and Degree $(F)=d$, then F is an algebraic extension of $\mathbf{Z}_p$ for some prime p; furthermore, for any $a\in F$, there is $h(t)\in\mathbf{Z}[t]$ such that $a+a^2h(a)=0$ and $\deg h(t)\leqq d$, on the other hand, there is $b\in F$ such that Degree $(b)=d$.

Now $[\mathbf{Z}_p(b): \mathbf{Z}_p]=d+1=$ the degree of the minimal polynomial of b over $\mathbf{Z}_p$. In fact $F=\mathbf{Z}_p(b)$. It is obvious that F contains $\mathbf{Z}_p(b)$. Let $a\in F$. If $a\notin\mathbf{Z}_p(b)$ then $(\mathbf{Z}_p(b))(a)\neq\mathbf{Z}_p(b)$. Now a being algebraic over $\mathbf{Z}_p$, $H=(\mathbf{Z}_p(b))(a)$ is a finite sub-

field of F and $[H: \mathbf{Z}_p]=n>d+1$. The field H is generated by one element c whose minimal polynomial over $\mathbf{Z}_p$ is of degree n. Thus Degree $(c)=n-1>d$, which is impossible. Therefore $F=\mathbf{Z}_p(b)$. Conversely, since F is a finite field of p^{d+1} elements, F is periodic. Now any $0\neq a\in F$ is algebraic over $\mathbf{Z}_p$ and $[\mathbf{Z}_p(a): \mathbf{Z}_p]=$ $=k\leqq d+1$. Thus the minimal polynomial of a is of degree at most $d+1$ and so Degree $(a)\leqq d$. Also F is generated by an element b such that Degree $(b)=d$.

Thus from Propositions 5 and 8 it follows that a periodic ring R whose Degree is d is such that $J(R)$ is nil and $R/J(R)$ is isomorphic to a subdirect sum of dense rings of algebraic linear transformations of vector spaces over $GF(p, k)$ with $k\leqq d+1$ for some primes p.

Proposition 9. *R is a periodic primitive ring and* Index $(R)=n$ *iff R is isomorphic to F_n (the ring of $n\times n$ matrices over F) for some algebraic extension F of $\mathbf{Z}_p$ for some prime p.*

Proof. Let F be an algebraic extension of $\mathbf{Z}_p$. If $A\in F_n$ then the matrix A has n^2 entries and involves only a finite number of elements of F. Thus $A\in G_n$ where G is a finite subfield of F, i.e. A belongs to a finite subring of F_n. By Theorem 1, F_n is periodic. It is well known that F_n is primitive. Since the minimal polynomial of $A\in F_n$ is of degree at most n, $N(F_n)\leqq n$. Also $A=[a_{ij}]$, $a_{ij}=1$ if $i<j$ and $a_{ij}=0$ if $i\geqq j$, satisfies $A^n=0$ and $A^{n-1}\neq 0$. Thus $N(F_n)=n$, and by Proposition 7, Index $(F_n)=N(F_n)=n$. Conversely, let R be a periodic primitive ring and Index $(R)=n$. Then $R\cong F_m$ or F_s is a homomorphic image of a subring of R, for every positive integer s, where F is an algebraic extension of $\mathbf{Z}_p$ for some p. Now, Index (R) does not increase by taking subrings or homomorphic images and so $s=$Index $(F_s)\leqq$ Index $(R)=n$. Thus $R\cong F_n$.

References

[1] I. N. Herstein, The structure of a certain class of rings, *Amer. J. Math.*, **75** (1953), 864—871.

[2] I. N. Herstein, *Non-Commutative Rings*, Carus Monograph Series, Math. Association of America (Menasha, Wis., 1968).

[3] A. A. Iskander, Locally finite ring varieties, *Proc. Amer. Math. Soc.*, **50** (1975), 28—32.

[4] N. Jacobson, *Structure of Rings*, Amer. Math. Soc. (Providence, 1964).

[5] R. L. Kruse, Identities satisfied by a finite ring, *J. Algebra*, **26** (1973), 298—318.

[6] I. V. L'vov, Varieties of associative rings. I, *Algebra i Logika*, **12** (1973), 269—297; English translation: pp. 150—167.

[7] I. V. L'vov, Varieties of associative rings. II, *Algebra i Logika*, **12** (1973), 667—688; English translation: pp. 381—393.

[8] J. M. Osborn, Varieties of algebras, *Advances in Math.*, **8** (1972), 163—369.

DEPARTMENT OF MATHEMATICS
OUWAIT UNIVERSITY
POBox 5486
KUWAIT